Consumers Union
Nonprofit Publisher of Consumer Reports

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE
CENTER FOR DEMOCRACY & TECHNOLOGY

November 7, 2011

By electronic mail

Secretary Diana Dooley
California Health and Human Services Agency
1600 Ninth Street, Room 460
Sacramento, California 95814

attn: Staci Gillespie
Office of Health Information Integrity

RE: CONSUMERS UNION'S AND CENTER FOR DEMOCRACY & TECHNOLOGY'S COMMENTS ON REVISED REGULATIONS FOR HIE DEMONSTRATION PROJECTS UNDER ASSEMBLY BILL 278

Dear Secretary Dooley:

Consumers Union[1] and the Center for Democracy & Technology[2] provide comment on the revised regulations governing health information exchange

[1] Consumers Union of United States, Inc., publisher of *Consumer Reports®*, is a non-profit membership organization chartered in 1936 to provide consumers with information, education, and counsel about goods, services, health, and personal finance. Consumers Union's publications have a combined paid circulation of approximately 8.3 million. These publications regularly carry articles reporting on Consumer Union's own product testing; on health, product safety, and marketplace economics; and on legislative, judicial, and regulatory actions that affect consumer welfare. Consumers Union derives its income solely from the sale of *Consumer Reports®*, its other publications and services, fees, noncommercial contributions and grants. Consumers Union's publications and services carry no outside advertising, and Consumers Union does not accept donations from corporations or corporate foundations.

[2] The Center for Democracy and Technology ("CDT") is a non-profit Internet and technology advocacy organization located in San Francisco, California, and Washington, D.C., which promotes public policies that preserve privacy and enhance civil liberties in the digital age. As information technology is increasingly used to support the exchange of medical records and other health information, CDT, through its Health Privacy Project, champions comprehensive privacy and security policies to protect health data. CDT promotes its positions through public policy advocacy, public education, and litigation, as well as through the development of industry best practices and technology standards. CDT plays an instrumental role in safeguarding consumer privacy on the Internet. Recognizing that a networked health care system can lead to improved health care quality, reduced costs, and empowered consumers, CDT is using its experience to shape workable privacy solutions for a health care system characterized by electronic health information exchange.

West Coast Office
1535 Mission Street
San Francisco, CA 94103
415.431.6747 tel
415.431.0906 fax
www.consumersunion.org

demonstration projects under Assembly Bill 278, 2010 Cal. Stat. ch. 227, released by the California Health and Human Services Agency on October 7, 2011 ("Revised Regulations"). We appreciate the efforts of the California Office of Health Information Integrity (CalOHII) to provide more clarity to the regulations. In particular, we are pleased to see the regulations provide a pathway for testing alternative privacy and security protections. It will be critical that this alternative process be robust and test one or more alternatives to protecting information that do not rely disproportionately on patient consent and that do not create disincentives to adopt electronic health records and electronic health information exchange.

However, as set forth in more detail below, the alternative process is not clear, and additional guidelines are needed to ensure a viable mechanism for testing alternatives and for evaluating those alternatives against the core approach for protecting privacy proposed in the regulations. We remain concerned that this core approach provides disincentives for the adoption of electronic health records and imposes a burden on both patients and providers that is not outweighed by the purported benefits for privacy. But if the core approach is subject to robust testing in the marketplace – and compared to other viable options – then the State of California will be better positioned to meet the intent of the legislature in enacting AB 278 and get evidence of what really works to protect privacy and enable electronic exchange of health information to improve individual and population health.

The bulk of our comments address the above issues, but we have also used this opportunity to make note of other aspects of the regulations that we believe warrant some attention. We thank you for the opportunity to provide these remarks.

Continuing Concerns with Core Approach Proposed in Regulations

We have on several previous occasions expressed our concerns with the core approach to privacy in these regulations. We understand the concerns of CalOHII about downstream uses of electronic health information, as set forth in detail in its white paper, "Analysis of the Risks Inherent in Implementing HIE Services & Strategies on How to Proceed in the Development of HIE Policies and Standards,"[3] and we appreciate the desire to give individuals some greater choices than the law already provides regarding whether their information can be initially disclosed in electronic form. But burdening the digital data flow at just the initiating point in the pipeline will not stop it from being digitized or further used downstream. As our prior comments have explained, the privacy benefits to the policy are negligible – but the potential burden on exchanges of information even for treatment purposes are considerable.

The revised regulations appear to expressly acknowledge that the core approach is focused merely on the initial disclosure. We note the new provision in section 126050(b), which states that after individual health information is disclosed through an HIO or independent directed exchange, it may be used or disclosed for any permitted purpose allowed by law that is specified in the Participant's Notice of Privacy Practices

[3] http://www.ohi.ca.gov/calohi/LinkClick.aspx?fileticket=Adh9MKWj0RU%3d&tabid=36

required by the HIPAA Privacy Rule. We interpret this to mean that CalOHII is seeking to regulate only the initial electronic disclosure of individual health information, and that participants receiving IHI need only abide by current law (and their own policies) with respect to any subsequent use and disclosure.[4] We agree that it makes sense not to require data recipients to treat data they receive differently based on the source, since this would be unduly burdensome (if not impossible) to manage. But the acknowledgement that downstream uses and disclosures are not reached by this policy underscores its limits in providing meaningful privacy protection for individuals. This makes all the more important the potential to test stronger protections by Requests to Develop Alternative Requirements.

We also note that the revised regulations make clear that consent is required even if the mechanism of exchange is through "independent directed exchange," which is "the electronic disclosure of encrypted individual health information over the internet to an unaffiliated entity and where third party facilitators do not have the ability to decrypt the content of the individual health information (IHI) package nor provide governance or oversight" (§ 126020(r)). There are no additional downstream privacy or security risks to exchange of information via this method, since the facilitator has no ability to access the underlying identifiable information, is acting at the direction of the data holder sending the information, and the information must be secured through encryption. A facilitating entity acting in this "conduit" capacity would not even be covered as a business associate under the HIPAA Privacy Rule.[5] This is a method of electronic transmission that CalOHII should favor – but instead such exchange is required to meet the same consent requirements as other forms of exchange that raise greater risks of downstream uses and are less familiar to patients. As explained in more detail below, we hope that CalOHII will, at a minimum, consider testing an approach which exempts independent directed exchange and exchange through HIOs that do not collect or access IHI from the opt-in consent requirements; individual consent or authorization would be required when required by existing state or federal law. Applicants should still be required to have in place specific policies to address the fair information practices (FIPs), including but not limited to how Applicants are going to effectively educate patients about electronic health information exchange.

We continue to urge CalOHII to focus its affirmative consent requirements on those HIO

---

[4] The regulations refer to such subsequent uses and disclosures by data recipients as "secondary" uses. Subsequent uses by a recipient of data from a participant are not necessarily "secondary" uses – they may in fact be uses for treatment, which are commonly referred to as primary. "Secondary use" typically describes uses of personal health information "outside of direct health care delivery," including analysis, research, quality and safety measurement, public health, payment, provider certification or accreditation, marketing, and other business applications, including strictly commercial activities." Safran, C., et al., "Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper," American Medical Informatics Association (2007), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2329823.

[5] "When a person or organization . . . acts merely as a conduit for personal health information, for example, the US Postal Service, certain private couriers, *or their electronic equivalents,*" a business associate relationship is not triggered and a business associate agreement is not required. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html. Adam Greene, who recently left the HHS Office of Civil Rights, recently opined that this exception also extends to entities that have access only to encrypted information. http://www.dwt.com/LearningCenter/Advisories?find=424711.

arrangements that would be most surprising to patients. As recommended by the Federal Health IT Policy Committee, these are HIOs where the decision to disclose a patient's individual health information is no longer in the control of the patient's trusted health care provider. Such arrangements are commonly found in centralized HIOs, or HIOs where a participating provider may freely access a patient's health information from another provider, as long as that accessing provider is operating in accordance with the general terms and conditions imposed on participants. We note that these revised rules include a definition of an HIO – but this definition does not focus on the types of HIOs that raise the most concern from a privacy and security standpoint. Merely facilitating exchange, or overseeing or governing it, does not raise additional privacy risk if the HIO does not access or maintain identifiable health information. The definitions of HIO and independent directed exchange should be crafted to clearly distinguish between those types of exchange arrangements that increase privacy risk to individuals and those that do not. CalOHII should then target its regulatory efforts to those arrangements that expose patients to increased privacy and security risks.

Requests to Develop Alternative Requirements (DAR)

We are very pleased to see CalOHII permitting demonstration project participants to seek approval to test alternative privacy and security policy requirements for their projects. However, we are concerned that the process for submitting such a request – and the standards under which such a request will be granted – are less than clear. Because the core requirements are a sharp departure from current state and federal privacy laws governing the exchange of health information, and given the importance of the public's interest in reaping the significant benefits of health information exchange, it is important that the demonstration projects simultaneously test a broader range of options for protecting privacy and achieving the goals of exchange.

However, we note that some of the factors that CalOHII has identified that it will use in judging DARs appear to be imposing standards that may be difficult to meet and, more importantly, standards which are not imposed on those who choose to use the core approach in the regulations. For example:

- DAR applicants must show, among other things, that disclosures are only to other CMIA providers with a treatment relationship with the patient, and that there is oversight and monitoring of disclosures, no re-purposing of the information, and control over the volume of information disclosed. These are all sound privacy and security safeguards, but it makes no sense to require these only for DAR applicants and not for core-approach applicants. Consent should not be an excuse not to require compliance with provisions like this, nor will obtaining the patient's affirmative consent overcome deficiencies in these areas.

- If de-identified data is being used or generated by a participant using DAR, the recipients of the data must be known to the participant. It is unclear why CalOHII has decided to impose this requirement only on DAR requesters. Given that de-

identified data is not regulated by either California or federal law, it may be difficult or impossible to know all of the downstream recipients.

- For independent directed exchanges, the information cannot contain sensitive health information (or information about another individual). Given that independent directed exchanges cannot, by definition, have access to IHI, and that exchange of sensitive information is already required to have authorization under California law in many instances, this exclusion makes little sense. As noted in more detail above, this type of electronic exchange raises little privacy and security risks and should be the preferred method of exchanging information, particularly when it is sensitive.

DAR applicants also must demonstrate that technology is not readily available to support compliance with the core approach. This point may be true, but CalOHII should be open to testing alternatives to the core approach without requiring an additional demonstration of technical infeasibility.

The core privacy approach in the regulations relies heavily on individual consent, notwithstanding that a growing number of agencies and privacy scholars agree that consent *per se* provides very weak privacy protection in practice.[6] In contrast, the DAR process may allow for the testing of approaches that place less emphasis on consent but provide strong privacy protections in practice. Subjecting all DAR applicants to these additional requirements makes little policy sense and may create disincentives for exchanges to test alternative approaches, frustrating the intent of the California legislature in enacting AB 278.

We urge CalOHII to establish a quick timeframe for turning around DAR requests, given the potential obstacles to exchange posed by the existing core requirements. CalOHII could promptly identify a number of alternative approaches to test through the DAR process, and leverage the resources of Cal eConnect to facilitate the review and approval of DARs. It is also critical that all approaches used by demonstration project participants be robustly evaluated for the degree to which they build public trust in health information exchange and the impact, if any, on the ease of exchange for the permitted purposes and on patient care generally.

---

[6] See "Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Businesses and Policymakers," Preliminary FTC Staff Report (December 2010) (hereinafter FTC Report), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; Fred Cate, "Looking Beyond Notice and Choice," BNA Privacy and Security Law Report (March 29, 2010), www.bna.com; Testimony of Marc Rotenberg, Executive Director, Electronic Privacy Information Center, before the U.S. Senate Commerce Committee (June 13, 2000), http://epic.org/privacy/internet/senate-testimony.html.

Other Issues to Consider

Making Consent More Meaningful

In circumstances where an individual's consent or authorization is sought, it is important that the consent be informed and meaningful. In our comments to the initial set of proposed regulations, we expressed concerns about the inadequacy of the consent process and provided suggestions on how to improve it. We note that those concerns were not addressed in this revised version, and we urge you to address this issue in subsequent versions.

It will always be important, for liability purposes, to have any required individual consents memorialized in writing. But for consent to truly be informed, it should never be reduced to a mere piece of paper. It should not be sufficient, for example, merely to hand the patient a multiple-page, single-spaced document minutes before the scheduled diagnosis or treatment or even to mail it to patients in advance of a visit or make it available for patients to read and "check the box" on a website.[7] The revised regulations still contain no requirement for providers or their staffs (the locus of trust for patients in information exchange) to have conversations with their patients; nor is there even a requirement that the notice and consent be presented in the primary language the patient reads and speaks—a substantial issue in California, where over one quarter of all Californians speak Spanish at home.

There are models for "meaningful" consent. Most recently, the Privacy and Security Tiger Team described the elements of meaningful consent. The patient should have knowledge and time in advance to make the decision whether to consent—for example, outside of the urgent need for care. Consent should not be compelled or used for discriminatory purposes—for example, consent to participate in a centralized HIO model or a federated HIO model should not be a pre-condition of receiving necessary medical services. The request for consent should include full transparency and education, ideally presented in a layered approach, so that patients first receive a clear and concise explanation of contemplated data sharing and the risks and benefits but have the option of learning more details.[8] The request for consent must be commensurate with the

---

[7] The research on the extent to which individuals read and understand consent forms or privacy policies is voluminous. For examples, see Priscilla Regan, The Role of Consent in Information Privacy Protection, in Considering Consumer Privacy: A Resource for Policy Makers and Practitioners, pg. 25 (Paula Bruening ed., 2003) (available at http://www.cdt.org/privacy/ccp/consentchoice2.shtml/pdf); Nathaniel Good, Rachna Dhamija, Jens Glokklags, David Tham, Steven Aronowitz, Deirdre Mulligan & Joseph Konstan, Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware (2005) (available at http://www.icsi.berkeley.edu/pubs/bcis/Spyware.pdf); Mark Hochhauser, Why Patients Won't Understand Their HIPAA Privacy Notices (Apr. 10, 2003) (available at http://www.privacyrights.org/ar/HIPAA-Readability.htm); Mark Hochhauser, Readability of HIPAA Privacy Notices, pgs. 5-6 (Mar. 12, 2003) (available at http://benefitslink.com/articles/hipaareadability.pdf).

[8] The layered notice approach was cited in the FTC's recent report on consumer privacy. FTC Report, supra note 3. An example can be found in the materials of the Markle Foundation applying the Markle Common Framework to sharing of clinical information with patients through an electronic health record "view and download" functionality. http://www.markle.org/health/publications-briefs-health/1201-policy-brief-download-

circumstances. For example, activities with information that are "new" to patients or that involve highly sensitive data should require greater degrees of education, time to make the decision, opportunity to discuss the question with the provider, etc.[9]

We also note that the revised regulations (§ 126055(b)(1)) introduce the concept of a "centralized consent registry," which is not defined in the regulations. We hope this does not suggest a consent process that takes place outside of the trusted relationship between the patient and the provider. Since survey data clearly shows that patients trust their health care providers with respect to their health information, instituting a consent process that takes the provider out of the equation could be antithetical to building trust in health information exchange.

Clarification of Security Requirements

We are pleased to see the regulations try to fill in some of the coverage gaps in the HIPAA Security Rule, such as by expressly requiring encryption and multi-factor authentication for remote access. However we also note that many of the security requirements in section 126070 that deal with safeguards for storing data apply to all participants even though some of them may not actually store personal health information (an HIO that merely facilitates exchange, for example, or an independent directed exchange). CalOHII should be clear about applying data storage security requirements only on those entities that will be collecting and maintaining identifiable health information.

Regulation of Business Associate Use of Information

The definition of the term "business associate agreement" deviates from the HIPAA definition and provides that the agreement specify the permitted uses and disclosures of individual health information" and require "appropriate safeguards to prevent the use or disclosure of the individual health information other than the permitted purposes specified in the agreement." This definition is more stringent than the provisions of the HIPAA Privacy Rule regarding business associate agreements, and suggests an attempt by CalOHII to address some of the deficiencies of the HIPAA Privacy Rule's regulation of business associates, as identified in CalOHII's the white paper.[10] However, the regulations do not take the step of expressly requiring participants to bind their business associates to specific use and disclosure terms. Requiring business associate agreements to specify the permitted uses and disclosures of health information is a more effective way than relying just on consent to address the potential for broader (and uncontemplated) downstream uses of health information, and we encourage CalOHII to pursue this policy – but we do not think it can be accomplished by merely changing the

---

capability.

[9] Letter from Health IT Policy Committee to David Blumenthal, pgs. 2-4 (Aug. 19, 2010). http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_6011_1815_17825_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/hitpc_transmittal_p_s_tt_9_1_10.pdf.

[10] Supra note 3. In the digest, CalOHII notes that further use or disclosure by a business associate must be performed under the expressed delegation of authority of a CMIA provider of health care (pg 15).

definition of "business associate agreement."

Scope of Regulations

Notwithstanding the improvements in clarity from the previous version, the regulations are still unclear regarding the scope of their coverage. The revised regulations include a new definition of participant, "a provider, health plan, [an HIO], or governmental authority approved by CalOHII to test privacy and security policies for the exchange of electronic health information," but the regulations themselves sometimes apply to "participants" (for example, §§ 126030, 126040(b)&(d), 126055), sometimes to "applicants" (for example, §§ 126040(a), 126060), or are generally worded without clarity as to whom they apply (for example, §§ 126040(c)(top), 126050). We read the informative digest to be clear that the rules are mandatory only for "entities selected to be demonstration project participants;" however, the regulatory text does not provide clarity on the distinction, if any, between applicants and participants, and does not consistently state who is responsible for complying with all of the provisions of the regulations. Without this clarity, moreover, we cannot be sure that we have identified all of the significant issues that the revised regulations might present.

HIPAA Preemption

We note that the revised regulations include a new section describing the circumstances under which a policy would not be preempted by HIPAA. We are not sure why CalOHII included this section, since we do not believe that a state agency – by fiat – can declare when HIPAA preemption does not apply. We are concerned that some of the examples could be confusing – for example, requirements that narrow the scope or duration of legal permissions provided by individuals for record access might not always be more protective than HIPAA, such as in the case of an individual authorizing downloads to his/her PHR. We suggest CalOHII be more clear about its intent in including this section, and if there is value to including it that outweighs the potential for confusion, clarify the examples.

Praise for Requiring Complaint Process, Prioritizing Complaints Reflecting Significant Privacy Risk

We thank you for continuing to include a requirement that participants establish a process to receive and respond to patient complaints, and for including in the revised regulations the requirement that complaints reflecting a significant risk to the privacy and confidentiality of individual health information be forwarded immediately to CalOHII.

Application of Trade Secret Provisions

The Revised Regulations introduce procedures should Applicants claim that some of the information included in the application is a trade secret. We wonder whether any material in the application might constitute a "trade secret." In any case, some of the provisions of section 126042 contravene the Public Record Act, Cal. Gov't Code §§

6250-6276.48, and must be revised.

Section 126042(a) provides that information in an application is not a public record if it "is designated to be a trade secret." On the contrary, mere designation as a trade secret does not make it so. Under the Uniform Trade Secret Act, the information must "[d]erive[] independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use" and be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[11] Where a regulatory filing designates some information as trade secret but it does not meet these requirements or the law instead classifies the information as a public record, then the information is a public record subject to mandatory disclosure.[12] Similarly, where CalOHII has denied protection as a trade secret, the information is a public record subject to disclosure. Contrary to proposed section 126042(a)(1), the Public Record Act does not permit an agency instead to make the record "exempt from disclosure under the Public Records Act during the time the records are in the possession" of the agency.

We also recommend that the proposed regulations explicitly make the request for trade secret exemption a public document, just as they provide for the request for confidentiality.

With respect to this proposed request for confidentiality, the revised regulations fail to cite the legal authority for such a request, and section 126042(c) provides no standard to govern the agency's determination. In the absence of such disclosure, it appears that the Public Records Act would again determine the standard and process. A request for confidentiality must show why particular information is exempt from disclosure under the Public Records Act. Absent such a showing and determination by the agency, the information is a public record subject to disclosure.

Conclusion

Thank you again for the opportunity to submit these comments.

Respectfully,

Mark Savage
Consumers Union of
United States

Deven McGraw
Center for Democracy
and Technology

[11] Cal. Civ. Code § 3426.1(d).

[12] See, e.g., State Farm Mutual Auto. Ins. Co. v. Garamendi, 32 Cal. 4th 1029 (2004).